CLAIMS

What is claimed is:

1. A method comprising:

monitoring a state of an image capture system (ICS) while it captures an image of a target;

making a digital record of the image;

certifying from the record of the image that no unauthorized material alteration of the state occurred during capture of the image.

2. The method of claim 1 further wherein certifying comprises:

encoding the record to allow detection of modification to the capture process and modification of the record itself.

3. The method of claim 1 wherein certifying comprises:

retaining a duplicate of the record of the image; and

preventing modification of the duplicate.

4. The method of claim 1 further comprising:

encrypting the record of the image.

5. The method of claim 1 further comprising:

incorporating markers of state in the record of the image.

6. The method of claim 1 further comprising:

preventing subsequent modification of the record of the image.

7. The method of claim 1 further comprising:

maintaining an audit log of access to the record of the image.

8. The method of claim 7 wherein maintaining the audit log comprises:

retaining a log record of at least one of who accessed the record of the image, a location of an accessor, when the record of the image was accessed, and what aspect of the record of the image was accessed.

9. The method of claim 7 wherein maintaining the audit log comprises:
maintaining a record of parties approving the record of the image.

10. The method of claim 1 further comprising:
retaining state information corresponding to the capture, wherein the state information includes at least one of: a time of event, an identification of the ICS, a network address of the ICS, a parameter of capture, a local access log and an automatically assigned index.

11. A computer readable storage media containing executable computer program instructions which when executed cause a digital processing system to perform a method comprising:
monitoring a state of an image capture system (ICS) while it captures an image of a target;
making a digital record of the image;
certifying from the record of the image that no unauthorized material alteration of the state occurred during capture of the image.

12. A method comprising:
monitoring a networked image capture system (ICS) while the ICS performs a capture of an image of a target;
making a digital record of the image;
certifying from the record of the image that no unauthorized material alteration of the state occurred during capture of the image.

13. The method of claim 12 further comprising:
automatically uploading data captured by the ICS to a remote node.

14. The method of claim 12 further comprising:
publishing the record of the image to a defined set of networked recipients.

15. The method of claim 12 further comprising:

maintaining an escrow copy of the data at a remote node secure from modification or destruction to guarantee an authenticity of the data.

16. The method of claim 12 further comprising:
defining access rights to the digital record of the image.

17. The method of claim 16 wherein access rights are automatically defined.

18. The method of claim 12 further comprising:
enabling the ICS from the remote node.

19. The method of claim 12 wherein the monitoring is performed from a remote node.

20. A computer readable storage media containing executable computer program instructions which when executed cause a digital processing system to perform a method comprising:
monitoring a networked image capture system (ICS) while the ICS performs a capture of an image of a target;
making a digital record of the image;
certifying from the record of the image that no unauthorized material alteration of the state occurred during capture of the image.

21. A method comprising:
preventing an unauthorized material alteration of a state of an image capture system (ICS) during a capture of an image of a target;
making a digital record of the image; and
preventing an unauthorized material alteration of data initially recorded in the record.

22. The method of claim 21 further comprising:
maintaining an audit log of access to the record of the image.

23. The method of claim 22 wherein maintaining the audit log comprises:

retaining a log record of at least one of who accesses the record of the image, a location of an accessor, when the record of the image was accessed and what aspect of the image record was accessed.

24. A computer readable storage media containing executable computer program instructions which when executed cause a digital processing system to perform a method comprising:

preventing an unauthorized material alteration of a state of an image capture system (ICS) during a capture of an image of a target;

making a digital record of the image; and

preventing an unauthorized material alteration of data initially recorded in the record.

25. A method comprising:

preventing an unauthorized material alteration of a state of a networked image capture system (ICS) during a capture of an image of a target;

making a digital record of the image; and

preventing an unauthorized material alteration of data initially recorded in the record of the image.

26. The method of claim 25 further comprising:

automatically uploading data captured by the ICS to a remote node.

27. The method of claim 25 further comprising:

maintaining an escrow copy of the data secure from modification or destruction to guarantee an authenticity of the data.

28. The computer readable storage media of claim 25 which when executed cause a digital processing system to perform a method further comprising:

preventing an unauthorized material alteration of a state of a networked image capture system (ICS) during a capture of an image of a target;

making a digital record of the image; and

preventing an unauthorized material alteration of data initially recorded in the record.

29. An apparatus comprising:

an image sensing array (ISA) disposed within an assembly; and

a data insertion device disposed within the assembly to modify a data stream corresponding to an image capture in a known way.

30. A method of claim 29 further comprising:

an encryption engine disposed within the assembly to encrypt the data stream within the assembly.

31. A method of claim 29 further comprising:

a tamper resistant assembly.

32. The apparatus of 29 further comprising:

a storage unit storing calibration data that defines a signature of inherent characteristics unique to the ISA.

33. The apparatus of claim 29 wherein the data insertion device comprises:

a light source positioned to illuminate a portion of the ISA in a known way during capture.

34. The apparatus of claim 29 wherein the data insertion device comprises:

a optical reference within the apparatus disposed to be imaged by the ISA as a precursor to capture of a target image.

35. The apparatus of claim 29 wherein the data insertion device comprises:

a reader to read pixels of the ISA masked from a field of view of the ISA to generate a pattern substantially unaffected by an image capture.

36. The apparatus of claim 29 wherein the data insertion device comprises:

a plurality of resistors defining a unique electrical signature.

37. The apparatus of claim 29 wherein the data insertion device comprises:

a memory retaining a marker data set for insertion in the data stream.